

\mathbb{F}_p -EXPRESSIBLE SUBALGEBRAS AND ORBITS OF $\mathbb{E}(r, \mathfrak{g})$

JARED WARNER

ABSTRACT. For G a connected, reductive group over an algebraically closed field k of large characteristic, we use the canonical Springer isomorphism between the nilpotent variety of $\mathfrak{g} := \text{Lie}(G)$ and the unipotent variety of G to study the projective variety of elementary subalgebras of rank r , denoted $\mathbb{E}(r, \mathfrak{g})$. In the case that G is defined over \mathbb{F}_p , we define the category of \mathbb{F}_p -expressible subalgebras of \mathfrak{g} , and prove that this category is isomorphic to Quillen's category of elementary abelian subgroups of the finite Chevalley group $G(\mathbb{F}_p)$. This isomorphism of categories leads to a correspondence between G -orbits of $\mathbb{E}(r, \mathfrak{g})$ defined over \mathbb{F}_p and G -conjugacy classes of elementary abelian subgroups of rank r in $G(\mathbb{F}_p)$. We use Magma to compute examples for $G = \text{GL}_n$, $n \leq 5$.

In [1], J. Carlson, E. Friedlander, and J. Pevtsova initiated the study of $\mathbb{E}(r, \mathfrak{g})$, the projective variety of rank r elementary subalgebras of a restricted lie algebra \mathfrak{g} . The authors demonstrate that the study of $\mathbb{E}(r, \mathfrak{g})$ informs the representation theory and cohomology of \mathfrak{g} . This is all reminiscent of the case of a finite group G , where the elementary abelian p -subgroups play a significant role in the story of the representation theory and cohomology of G , as first explored by Quillen in [14].

In this paper, we further explore the structure of $\mathbb{E}(r, \mathfrak{g})$ and its relationship with elementary abelian subgroups. Theorem 3.12 shows in the case that $\mathfrak{g} = \text{Lie}(G)$, the category of \mathbb{F}_p -expressible subalgebras (Definitions 2.2 and 3.2) is isomorphic to Quillen's category of elementary abelian p -subgroups of $G(\mathbb{F}_p)$. The proof of Theorem 3.12 relies on the canonical Springer isomorphism $\sigma : \mathcal{N}(\mathfrak{g}) \rightarrow \mathcal{U}(G)$, which has been shown to exist under certain hypotheses, as detailed in [8], [2], [12], and [5]. Together with Lang's theorem, Theorem 3.12 implies Theorem 4.3, which establishes a natural bijection between the G -orbits of $\mathbb{E}(r, \mathfrak{g})$ defined over \mathbb{F}_p and the G -conjugacy classes of elementary abelian subgroups of rank r in $G(\mathbb{F}_p)$. Example 4.7, due to R. Guralnick, shows that $\mathbb{E}(r, \mathfrak{g})$ may be an infinite union of G -orbits. Our interest in describing the G -orbits is motivated by the results of §6 in [1], where the authors construct algebraic vector bundles on G -orbits of $\mathbb{E}(r, \mathfrak{g})$ associated to a rational G -module M via the restriction of image, cokernel, and kernel sheaves.

A question of E. Friedlander's asks for conditions implying that $\mathbb{E}(r, \mathfrak{g})$ is irreducible. In the case that $\mathfrak{g} = \mathfrak{gl}_n$, Theorem 5.1 reports certain ordered pairs (r, n) for which $\mathbb{E}(r, \mathfrak{g})$ is irreducible. This theorem relies on previous results concerning the irreducibility of the variety of r -tuples of pair-wise commuting, nilpotent matrices (see [10] for a nice summary of these results).

Date: February 25, 2014.

2010 Mathematics Subject Classification. 17B45, 20G40.

Key words and phrases. restricted Lie algebras, Springer isomorphisms.

Finally, in §6, we compute a few examples for $G = \mathrm{GL}_n$. Proposition 6.3 computes the dimension of the open orbit defined by a regular nilpotent element, as first considered in Proposition 3.19 of [1]. For $n \leq 5$, we report the number of G -orbits in $\mathbb{E}(r, \mathfrak{gl}_n)$ and their dimensions. These computations depend on Conjecture 6.1, which supposes the dimension of an orbit is related to the size of the corresponding G -conjugacy class.

Acknowledgements. We would like to thank Eric Friedlander, whose support and guidance were central throughout the research and writing of this paper. In particular, Eric's contributions include, but are not limited to, the suggestion to use Springer isomorphisms to study elementary subalgebras and the idea to apply Lang's theorem in the proof of Theorem 4.3. Paul Sobaje is also due our gratitude for explaining the history and development of the canonical Springer isomorphism. Finally, we would like to thank Robert Guralnick for pointing out that not all orbits of an action defined over \mathbb{F}_p will themselves be defined over \mathbb{F}_p , and for contributing Example 4.7.

1. REVIEW AND PRELIMINARIES

Let k be an algebraically closed field of characteristic $p > 0$, and let G be a connected, reductive algebraic group over k . Assume also that $p \geq h$, where h is the Coxeter number of G , and that p is very good for G (note that the 'very good' condition is redundant in all cases except when $p = h$ and G has an adjoint component of type A , PSL_p). The unipotent elements of G form an irreducible closed subvariety of G , denoted $\mathcal{U}(G)$, and G acts by conjugation on $\mathcal{U}(G)$. In the Lie algebra setting, the nilpotent elements of $\mathfrak{g} := \mathrm{Lie}(G)$ also form an irreducible closed subvariety of \mathfrak{g} , denoted $\mathcal{N}(\mathfrak{g})$, and $\mathcal{N}(\mathfrak{g})$ is a G -variety under the adjoint action of G on \mathfrak{g} . The main tool we will use to translate information between the group and Lie algebra settings will be a well-behaved Springer isomorphism.

Definition 1.1. A *Springer isomorphism* is a G -equivariant isomorphism of algebraic varieties $\sigma : \mathcal{N}(\mathfrak{g}) \rightarrow \mathcal{U}(G)$.

A note of Serre in ([5], §10) mentions that if p is very good for G , then Springer isomorphisms exist, but are not unique. In fact, they are parametrized by a variety of dimension equal to $\mathrm{rank}(G)$.

Example 1.2 ([13], §3). Let $G = \mathrm{SL}_n$. Then the Springer isomorphisms are parameterized by the variety $a_1 \neq 0$ in \mathbb{A}^{n-1} by

$$\sigma_{(a_1, \dots, a_{n-1})}(X) = 1 + a_1 X + \dots + a_{n-1} X^{n-1}$$

where $X^n = 0$. It follows that different Springer isomorphisms can behave very differently. Here, since $p \geq h(\mathrm{SL}_n) = n$, we have the particularly nice choice of Springer isomorphism

$$\sigma(X) = 1 + X + \frac{X^2}{2!} + \dots + \frac{X^{p-1}}{(p-1)!}$$

This is just the truncated exponential series, which we will denote \exp .

The truncated exponential series considered in Example 1.2 has the following convenient property for $p \geq n$:

$$(1.2.1) \quad [X, Y] = 0 \implies \exp(X + Y) = \exp(X) \exp(Y)$$

We give a brief proof of (1.2.1). Serre records in ([9], (4.1.7)) that the following formula holds in general:

$$(1.2.2) \quad [X, Y] = 0 \implies \exp(X)\exp(Y) = \exp(X + Y - W_p(X, Y))$$

where $W_p(X, Y) = \frac{1}{p}((X + Y)^p - X^p - Y^p)$. For $p \geq n$, with X and Y commuting nilpotent matrices, we have $X^p = Y^p = (X + Y)^p = 0$ so that $W_p(X, Y) = 0$ and we recover (1.2.1).

Proposition 5.3 in [8] states for any parabolic subgroup P in G whose unipotent radical U_P has nilpotence class less than p , there is a unique P -equivariant isomorphism $\varepsilon_P : \mathfrak{u}_P \rightarrow U_P$ satisfying the following conditions.

- (1) ε_P is an isomorphism of algebraic groups, where \mathfrak{u}_P has the structure of an algebraic group via the Baker-Campbell-Hausdorff formula (notice the condition on the nilpotence class of \mathfrak{u}_P is required for this group law to make sense).
- (2) The differential of ε_P is the identity on \mathfrak{u}_P .

In Theorem 3 of [2], the authors uniquely extend this isomorphism on \mathfrak{u}_P to all of $\mathcal{N}(\mathfrak{g})$, with weaker conditions on p than we consider in this paper. Under our assumptions on p , their result implies the following theorem.

Theorem 1.3. *For G a connected, reductive algebraic group, and for $p \geq h(G)$, p very good, there is a (necessarily) unique Springer isomorphism $\sigma : \mathcal{N}(\mathfrak{g}) \rightarrow \mathcal{U}(G)$ which restricts to the canonical isomorphism of [8] on all \mathfrak{u}_P for P any parabolic subgroup of G .*

This canonical Springer isomorphism shares the same property enjoyed by the truncated exponential:

$$(1.3.1) \quad [X, Y] = 0 \implies \sigma(X + Y) = \sigma(X)\sigma(Y)$$

To see this, suppose X and Y are commuting nilpotent elements. Lemma 9.7 in [6] shows that there is some Borel subgroup of G with unipotent radical U such that $X, Y \in \text{Lie}(U)$. It follows by Theorem 1.3 that $\sigma(X \star Y) = \sigma(X)\sigma(Y)$, where \star is the group operation defined by the Baker-Campbell-Hausdorff formula, which for commuting elements satisfies $X \star Y = X + Y$. Property (1.3.1) follows.

We will use the canonical Springer isomorphism σ to study the projective variety $\mathbb{E}(r, \mathfrak{g})$, as defined in [1]. The following discussion is relevant for an arbitrary restricted Lie algebra $(\mathfrak{g}, [p])$, but we are only concerned with the case $\mathfrak{g} = \text{Lie}(G)$.

Definition 1.4 ([1], Definition 1.2). An *elementary subalgebra* $\epsilon \subset \mathfrak{g}$ is an abelian Lie subalgebra of \mathfrak{g} with trivial restriction, i.e., $x^{[p]} = 0$ for all $x \in \epsilon$.

Let $\mathbb{E}(r, \mathfrak{g})$ be the set of elementary subalgebras of rank r in \mathfrak{g} . Considering $\epsilon \hookrightarrow \mathfrak{g}$ as an inclusion of vector spaces, there is an embedding $\mathbb{E}(r, \mathfrak{g}) \hookrightarrow \text{Grass}(r, \mathfrak{g})$. This is a closed embedding so that $\mathbb{E}(r, \mathfrak{g})$ has the structure of a projective subvariety of $\text{Grass}(r, \mathfrak{g})$ ([1], Proposition 1.3). If \mathfrak{g} is the Lie algebra of an algebraic group G , then $\mathbb{E}(r, \mathfrak{g})$ is a G -variety via the adjoint action of G on \mathfrak{g} . Specifically, for any $\epsilon \in \mathbb{E}(r, \mathfrak{g})$ and any $g \in G$, the image of ϵ under $\text{Ad}_g : \mathfrak{g} \rightarrow \mathfrak{g}$ is elementary of rank r .

We note for later purposes the following construction, which appear in Proposition 1.3 of [1] and its proof. Let $\mathcal{C}_r(\mathcal{N}(\mathfrak{g}))^\circ$ denote the variety of r -tuples of pairwise-commuting, nilpotent, linearly independent elements of \mathfrak{g} . By taking the k -span

of elements in an r -tuple, any $(X_1, \dots, X_r) \in \mathcal{C}_r(\mathcal{N}(\mathfrak{g}))^\circ$ defines an elementary subalgebra of rank r , so there is a map of algebraic varieties $\mathcal{C}_r(\mathcal{N}(\mathfrak{g}))^\circ \rightarrow \mathbb{E}(r, \mathfrak{g})$.

2. \mathbb{F}_p -EXPRESSABILITY AND \mathbb{F}_p -RATIONAL POINTS OF $\mathbb{E}(r, \mathfrak{g})$

The following definitions are motivated by ([2], §3). As before, let G be a connected, reductive algebraic group over k , but in all that follows suppose that G has a fixed \mathbb{F}_p -structure. In other words, suppose there is some algebraic group G_0 over \mathbb{F}_p such that $G = G_0 \times_{\mathbb{F}_p} \text{Spec } k$. It follows that $\mathfrak{g} := \text{Lie}(G)$ has an \mathbb{F}_p -structure coming from $\mathfrak{g}_0 := \text{Lie}(G_0)$ given by $\mathfrak{g} = \mathfrak{g}_0 \times_{\mathbb{F}_p} \text{Spec } k$. We write $G(\mathbb{F}_p)$ ($\mathfrak{g}(\mathbb{F}_p)$) to denote the \mathbb{F}_p -rational points of G (\mathfrak{g}), or more precisely, the k -points of G (\mathfrak{g}) obtained by base-changing an \mathbb{F}_p -point of G_0 (\mathfrak{g}_0). Here, we view the vector space \mathfrak{g} as a scheme over k via the following standard construction. Given a finite dimensional vector space V over k , give V the structure of a linear scheme over k with coordinate algebra $S^*(V^\#)$. Then the k -points of V with this scheme structure are naturally identified with the elements of the vector space V . In particular, in the setting just discussed, $\mathfrak{g}(\mathbb{F}_p) \cong \mathfrak{g}_0$.

Definition 2.1 ([2], §3, Definition 1). An element $X \in \mathfrak{g}$ is \mathbb{F}_p -expressible if it can be written as $X = \sum c_i X_i$ with $c_i \in k$, $X_i \in \mathfrak{g}(\mathbb{F}_p)$, $X_i^{[p]} = 0 = [X_i, X_j]$.

This definition can be extended to the notion of an \mathbb{F}_p -expressible subalgebra.

Definition 2.2. We call an elementary subalgebra ϵ an \mathbb{F}_p -expressible subalgebra, if it has an \mathbb{F}_p -expressible basis, that is, a basis of the form $\{X_1, \dots, X_r\} \subset \mathfrak{g}(\mathbb{F}_p)$.

To speak of \mathbb{F}_p -rational points of $\mathbb{E}(r, \mathfrak{g})$, we require a rationality condition on \mathfrak{g} .

Lemma 2.3. If \mathfrak{g} has an \mathbb{F}_p -structure given by $\mathfrak{g} = \mathfrak{g}_0 \otimes_{\mathbb{F}_p} k$, then $\mathbb{E}(r, \mathfrak{g})$ is defined over \mathbb{F}_p .

Proof. Fix an embedding $\mathfrak{g}_0 \hookrightarrow \mathfrak{gl}_n(\mathbb{F}_p)$. Then $\mathfrak{g} \hookrightarrow \mathfrak{gl}_n$ is determined by linear equations with coefficients in \mathbb{F}_p . The equations defining the nilpotent, commuting, and linearly independent conditions are all homogeneous polynomials with coefficients in \mathbb{F}_p as well. \square

The following identification of the rational points of $\mathbb{E}(r, \mathfrak{g})$ will prove useful later.

Proposition 2.4. The \mathbb{F}_p -rational points of $\mathbb{E}(r, \mathfrak{g})$ are precisely the \mathbb{F}_p -expressible subalgebras of \mathfrak{g} .

Proof. First, notice that $\mathbb{E}(r, \mathfrak{g})(\mathbb{F}_p) = \mathbb{E}(r, \mathfrak{g}) \cap \text{Grass}(r, \mathfrak{g})(\mathbb{F}_p)$. The result follows from the fact that the \mathbb{F}_p -rational points of the Grassmannian are those r -planes with a basis in $\mathfrak{g}(\mathbb{F}_p)$. \square

We conclude this section by noting another property of the canonical Springer isomorphism σ given by Theorem 1.3. In Theorem 3 of [2], the authors note that in the case that G is defined over \mathbb{F}_p , σ is also defined over \mathbb{F}_p . That is, there is a morphism $\sigma_0 : \mathcal{N}(\mathfrak{g}_0) \rightarrow \mathcal{U}(G_0)$ such that $\sigma = \sigma_0 \times_{\mathbb{F}_p} \text{id}_{\text{Spec } k}$.

3. AN ISOMORPHISM OF CATEGORIES

We begin by recalling the category of elementary abelian p -subgroups of a finite group, first considered by Quillen. For $g \in G$, let $c_g : G \rightarrow G$ be defined by $c_g(h) = ghg^{-1}$.

Definition 3.1. Let G be a finite group, and let p be a prime dividing the order of G . Define \mathcal{C}_G to be the category whose objects are the elementary abelian p -subgroups of G , and whose morphisms are inclusions composed with c_g for some $g \in G$. In particular we have a morphism $E \rightarrow E'$ if and only if E is conjugate to a subgroup of E' .

Motivated by this definition, we make similar definitions for restricted Lie algebras.

Definition 3.2.

- (1) Let G be an algebraic group defined over k , and let $\mathfrak{g} = \text{Lie}(G)$. Define $\mathcal{C}_{\mathfrak{g}}$ to be the category whose objects are the elementary abelian subalgebras of \mathfrak{g} , and whose morphisms are inclusions followed by Ad_g for $g \in G$.
- (2) Inside of $\mathcal{C}_{\mathfrak{g}}$, let $\mathcal{C}_{\mathfrak{g}}(\mathbb{F}_p)$ be the subcategory whose objects are \mathbb{F}_p -expressible subalgebras, and whose morphisms are inclusions composed with Ad_g for $g \in G(\mathbb{F}_p)$.

The main result of this section is Theorem 3.12, which establishes an isomorphism between the categories $\mathcal{C}_{G(\mathbb{F}_p)}$ and $\mathcal{C}_{\mathfrak{g}}(\mathbb{F}_p)$. Before proving the theorem, we develop the necessary machinery using σ , the canonical Springer isomorphism as discussed in §1. We begin with a small technical lemma about fields of definition that will be needed later.

Lemma 3.3. *Let K/k be a field extension, and let V be a finite dimensional vector space over K . Choose a basis e_1, e_2, \dots, e_n of V to identify V with K^n . Let $\{u_1, \dots, u_r\}, \{v_1, \dots, v_r\} \subset K^n$ be so that the span of the u_i 's over K equals the span of the v_i 's over K . Then*

$$\text{Span}_k\{u_1, \dots, u_r\} = \text{Span}_k\{v_1, \dots, v_r\}$$

Proof. First of all, by the uniqueness of the reduced form of a matrix, notice that a subset $S \subset K^n$ is K -linearly dependent if and only if it is k -linearly dependent.

Next, notice that the containment

$$\text{Span}_K\{u_1, \dots, u_r\} \subset \text{Span}_K\{v_1, \dots, v_r\}$$

holds if and only if $\{v_1, \dots, v_r, u_i\}$ is linearly dependent over K for all i . By our first observation, this is equivalent to $\{v_1, \dots, v_r, u_i\}$ being linearly dependent over k for all i , which is equivalent to the containment

$$\text{Span}_k\{u_1, \dots, u_r\} \subset \text{Span}_k\{v_1, \dots, v_r\}$$

□

Now, for any $g \in \mathcal{U}(G)$ and any $c \in k$, define $g^c = \sigma(c\sigma^{-1}(g))$. We will use σ to map rank r elementary subalgebras to rank r elementary abelian subgroups and the following notion of independence in the group setting will help ensure that the rank is preserved.

Definition 3.4. Let G be a connected, reductive group. We say that pairwise commuting elements $g_1, \dots, g_r \in \mathcal{U}(G)$ are *multiplicatively independent* if whenever $\prod g_i^{c_i} = e$ then $c_i = 0$ for $i = 1, \dots, r$.

Example 3.5. Note that the definition of multiplicative independence implies that the g_i generate (in a group-theoretic sense) an elementary abelian subgroup of rank

r , but the converse is not true in general. For instance, let $p = 2$, and consider the matrices

$$g_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, g_2 = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_4)$$

where $x \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Then g_1 and g_2 are commuting unipotent elements, and they generate an elementary abelian subgroup of rank 2 in $\mathrm{SL}_2(k)$. In this example, σ is the truncated exponential, and σ^{-1} the truncated logarithm, so one can check that we have:

$$g_1^x g_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^x \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

so that g_1 and g_2 are not multiplicatively independent.

Lemma 3.6. *The pairwise commuting elements $X_1, \dots, X_r \in \mathcal{N}(\mathfrak{g})$ are linearly independent if and only if the pairwise commuting elements $\sigma(X_1), \dots, \sigma(X_r) \in \mathcal{U}(G)$ are multiplicatively independent.*

Proof. Suppose that $X_1, \dots, X_r \in \mathfrak{g}$ are linearly independent and $e = \prod \sigma(X_i)^{c_i}$. By (1.3.1), we have $e = \prod \sigma(X_i)^{c_i} = \prod \sigma(c_i X_i) = \sigma(\sum c_i X_i)$. It follows by the injectivity of σ that $0 = \sum c_i X_i$ so that $c_i = 0$ for all i . The steps are all reversible. \square

Corollary 3.7. *If $\epsilon = \mathrm{Span}_k\{X_1, \dots, X_r\}$ is an elementary subalgebra of rank r , then $E = \langle \sigma(X_1), \dots, \sigma(X_r) \rangle$ is an elementary abelian subgroup of rank r .*

Proof. If $\epsilon = \mathrm{Span}_k\{X_1, \dots, X_r\}$ is an elementary subalgebra of rank r , then, the pairwise commuting, nilpotent, and linear independent conditions for $\{X_1, \dots, X_r\}$ translate to pairwise commuting, unipotent, and multiplicatively independent conditions for $\{\sigma(X_1), \dots, \sigma(X_r)\}$. As noted in Example 3.5, the multiplicative independence of r pairwise commuting unipotent elements implies the subgroup they generate is elementary abelian of rank r . \square

Notice that in general the converse of Corollary 3.7 is not true. Example 3.5 shows that the group $\langle g_1, g_2 \rangle$ is elementary abelian of rank 2, but the elementary subalgebra $\mathrm{Span}\{\sigma^{-1}(g_1), \sigma^{-1}(g_2)\}$ has rank 1. We now use Lemma 3.3 to show that this drop in rank does not occur for subgroups in $G(\mathbb{F}_p)$.

Lemma 3.8. *If $g_1, \dots, g_r \in G(\mathbb{F}_p)$ are pairwise commuting, unipotent elements which generate an elementary abelian subgroup of rank r , then they are multiplicatively independent. In particular, if $E = \langle g_1, \dots, g_r \rangle \subset G(\mathbb{F}_p)$ is elementary abelian of rank r , then the \mathbb{F}_p -expressible subalgebra $\epsilon = \mathrm{Span}\{\sigma^{-1}(g_1), \dots, \sigma^{-1}(g_r)\}$ is elementary of rank r .*

Proof. Suppose $e = \prod g_i^{c_i}$. Then $0 = \sum c_i \sigma^{-1}(g_i)$ with $\sigma^{-1}(g_i) \in \mathfrak{g}(\mathbb{F}_p)$. If some c_i is non-zero, then the proof of Lemma 3.3 shows we may take the c_i to be in \mathbb{F}_p . This contradicts the fact that the g_i generate an elementary abelian subgroup of rank r . The proof of the second statement is similar to the proof of Corollary 3.7, where we now know that the generators of a rank r subgroup in $G(\mathbb{F}_p)$ are multiplicatively independent, and therefore map to r linearly independent vectors in $\mathfrak{g}(\mathbb{F}_p)$ under σ^{-1} . \square

We would like to show that this process of moving between subalgebras and subgroups is independent of any choice of generators or basis. In general, this is not true. Again, we find a counterexample from Example 3.5. The matrices $\sigma^{-1}(g_1) = g_1 - I_2$ and $\sigma^{-1}(g_2) = g_2 - I_2$ both span the same rank 1 elementary subalgebra, but g_1 and g_2 generate different subgroups in G . However, as a result of Lemma 3.3, we do obtain a one-to-one correspondence between \mathbb{F}_p -expressible subalgebras and elementary abelian subgroups in $G(\mathbb{F}_p)$ which is independent of any choice.

Lemma 3.9. *Suppose ϵ is an \mathbb{F}_p -expressible elementary subalgebra of rank r , with \mathbb{F}_p -expressible bases $\{X_1, \dots, X_r\}$ and $\{Y_1, \dots, Y_r\}$. Then $\langle \sigma(X_1), \dots, \sigma(X_r) \rangle = \langle \sigma(Y_1), \dots, \sigma(Y_r) \rangle$.*

Similarly, if $E = \langle g_1, \dots, g_r \rangle = \langle h_1, \dots, h_r \rangle \subset G(\mathbb{F}_p)$ is an elementary abelian p -group of rank r , then $\text{Span}\{\sigma^{-1}(g_1), \dots, \sigma^{-1}(g_r)\} = \text{Span}\{\sigma^{-1}(h_1), \dots, \sigma^{-1}(h_r)\}$.

Proof. By symmetry, it suffices to show one containment. Let $Y_i = \sum c_{ij} X_j$ where the $c_{ij} \in \mathbb{F}_p$ by Lemma 3.3. Then

$$\sigma(Y_i) = \prod \sigma(X_j)^{c_{ij}} \in \langle \sigma(X_1), \dots, \sigma(X_r) \rangle$$

Similarly, suppose $h_i = \prod (g_j)^{c_{ij}}$, with $c_{ij} \in \mathbb{F}_p$. Then $\sigma^{-1}(h_i) = \sum c_{ij} \sigma^{-1}(g_j)$. \square

Remark 3.10. With the definition $g^c = \sigma(c\sigma^{-1}(g))$ for unipotent g and $c \in k$, we could remove the rationality hypotheses in Lemma 3.9 if we define the subgroup generated by g_1, \dots, g_r in a different way. For any subfield $k' \subset k$, and any pairwise commuting nilpotent elements g_i , define:

$$\langle g_1, \dots, g_r \rangle_{k'} = \left\{ \prod_{i=1}^r g_i^{c_i} \mid c_i \in k' \right\}$$

Notice that $\langle g_1, \dots, g_r \rangle_{\mathbb{F}_p} = \langle g_1, \dots, g_r \rangle$, where for the right-hand side we use the usual group-theoretic notion of generation. With our generalized definition, it is true that the map sending the subalgebra $\text{Span}_{k'}\{X_1, \dots, X_r\}$ to the subgroup $\langle \sigma(X_1), \dots, \sigma(X_r) \rangle_{k'}$ is a bijection, independent of any choice. The disadvantage in this approach is that the subgroup $\langle \sigma(X_1), \dots, \sigma(X_r) \rangle_{k'}$ has infinite rank if k' is infinite, and we are interested in finite subgroups of the finite group $G(\mathbb{F}_p)$.

By Lemma 3.9, we have a natural and well-defined process of moving between subgroups and subalgebras.

Definition 3.11. Given an r -dimensional, \mathbb{F}_p -expressible elementary subalgebra $\epsilon \subset \mathfrak{g}$, define an elementary abelian p -group of rank r , $\Sigma(\epsilon) \subset G(\mathbb{F}_p)$, as follows: choose an \mathbb{F}_p -expressible basis, $\{X_1, \dots, X_n\}$, and let $\Sigma(\epsilon) := \langle \sigma(X_1), \dots, \sigma(X_r) \rangle$. Similarly, given an elementary abelian p -subgroup of rank r , $E \subset G(\mathbb{F}_p)$, define an r -dimensional \mathbb{F}_p -expressible elementary subalgebra, $\Sigma^{-1}(E) \subset \mathfrak{g}$, as follows: choose generators $\langle g_1, \dots, g_r \rangle$, and let $\Sigma^{-1}(E) := \text{Span}_k\{\sigma^{-1}(g_1), \dots, \sigma^{-1}(g_r)\}$. By Lemma 3.9, these definition are independent of any choice.

Notice that the maps defined above are inverses of each other, which leads to the main result of this section.

Theorem 3.12. *Let G be a reductive, connected group, and suppose $p \geq h(G)$, and p is very good for G . Then the categories $\mathcal{C}_{G(\mathbb{F}_p)}$ and $\mathcal{C}_{\mathfrak{g}}(\mathbb{F}_p)$ are isomorphic.*

Proof. Define a functor $\Sigma : \mathcal{C}_{\mathfrak{g}}(\mathbb{F}_p) \rightarrow \mathcal{C}_{G(\mathbb{F}_p)}$ which on objects is given by $\Sigma(\epsilon)$. For morphisms, notice that by Definition 3.11, there is an inclusion $\iota : \epsilon \hookrightarrow \epsilon'$ if and only if there is an inclusion $\Sigma(\iota) : \Sigma(\epsilon) \hookrightarrow \Sigma(\epsilon')$ (after choosing an \mathbb{F}_p -expressible basis for ϵ , extend to an \mathbb{F}_p -expressible basis for ϵ'). Finally, for any $g \in G(\mathbb{F}_p)$, define $\Sigma(\text{Ad}_g) : \Sigma(\epsilon) \rightarrow \Sigma(\text{Ad}_g(\epsilon))$ by $\Sigma(\text{Ad}_g)(\sigma(X_i)) := \sigma(\text{Ad}_g(X_i)) = g\sigma(X_i)g^{-1}$, where $\{X_1, \dots, X_r\}$ is an \mathbb{F}_p -expressible basis of ϵ . Notice here we have used the G -equivariance of σ . The inverse functor of Σ is constructed using Σ^{-1} on objects, and a similar process on morphisms, relying on the G -equivariance of σ . \square

Example 3.13. Let $G = SO_3$, $p \geq 3$, and $r = 1$. A skew-symmetric 3×3 nilpotent matrix has the form:

$$\begin{pmatrix} 0 & x & y \\ -x & 0 & z \\ -y & -z & 0 \end{pmatrix}$$

where $x^2 + y^2 + z^2 = 0$. It follows that $\mathbb{E}(1, \mathfrak{so}_3)$ is the irreducible projective variety in \mathbb{P}^2 of all points $[x : y : z]$ satisfying $x^2 + y^2 + z^2 = 0$. This equation has p^2 solutions over \mathbb{F}_p (exercise!), one of which is $(0, 0, 0)$. This leaves us with a set S of $p^2 - 1$ non-trivial solutions, each of which spans a one dimensional \mathbb{F}_p -expressible subalgebra. Each \mathbb{F}_p -expressible subalgebra contains exactly $p - 1$ elements of S , so that there are $p + 1$ different \mathbb{F}_p -expressible subalgebras. It is also true that there are $p + 1$ subgroups of the form $\mathbb{Z}/p\mathbb{Z}$ in $SO_3(\mathbb{F}_p)$, as we expect from Theorem 3.12.

Remark 3.14. In this section we have chosen to use Quillen's category of elementary abelian subgroups as a motivation for defining our category of elementary subalgebras. Our reasoning behind this is due to the importance of Quillen's category in the cohomology of the group $G(\mathbb{F}_p)$. It is the author's hope that the isomorphic category $\mathcal{C}_{\mathfrak{g}}(\mathbb{F}_p)$ or the larger category $\mathcal{C}_{\mathfrak{g}}$ might hold a similar importance in the cohomology of \mathfrak{g} .

Another approach for this section would be to motivate our definitions by the Quillen complex of elementary abelian subgroups, that is, the complex associated to the poset of elementary abelian subgroups of G ordered by inclusion. With a similar definition of the complex of elementary subalgebras, we find that Quillen's complex for $G(\mathbb{F}_p)$ is isomorphic to the subcomplex of \mathbb{F}_p -expressible subalgebras. Using the appropriate analogues of group-theoretic notions (for example, the Frattini subalgebra of \mathfrak{g} as studied in [4]), much of the machinery developed in Part 2 of [11] for groups can be developed for Lie algebras. In particular, it is true that the subcomplex of p -subalgebras is G -homotopy equivalent to the subcomplex of elementary subalgebras, and the proof follows that of the analogous statement for groups (see ([11], Theorem 4.2.4) for a proof using Quillen's Fiber Theorem). It might also be the case that we can learn something about Lie algebra cohomology from this perspective.

4. G -ORBITS OF $\mathbb{E}(r, \mathfrak{g})$ DEFINED OVER \mathbb{F}_p

In this section we use Lang's theorem to show that \mathbb{F}_p -rational points exist in the G -orbits of $\mathbb{E}(r, \mathfrak{g})$ that are defined over \mathbb{F}_p . By the previous sections, these points correspond exactly to elementary abelian p -groups of rank r in $G(\mathbb{F}_p)$. This leads to Theorem 4.3, which gives a bijection between the G -orbits of $\mathbb{E}(r, \mathfrak{g})$ defined over \mathbb{F}_p and G -conjugacy classes of elementary abelian p -subgroups of rank r in $G(\mathbb{F}_p)$. We clarify the phrase " G -conjugacy classes of elementary abelian p -groups of rank

r in $G(\mathbb{F}_p)$.” Two elementary abelian p -subgroups of rank r in $G(\mathbb{F}_p)$, say E_r and E'_r , are G -conjugate if there is $g \in G(k)$ such that g conjugates E_r to E'_r . Notice this is not the same as the standard notion of conjugate subgroups in $G(\mathbb{F}_p)$, as there may be non-conjugate subgroups $H, K \subset G(\mathbb{F}_p)$ which are conjugate when viewed as subgroups in $G(\mathbb{F}_q)$ for $q = p^d$.

E. Friedlander has asked for sufficient conditions such that $\mathbb{E}(r, \mathfrak{g})$ is a finite union of G -orbits. Theorem 4.3 shows that if G is connected and reductive, and if $p \geq h(G)$, p very good, then $\mathbb{E}(r, \mathfrak{g})$ has finitely many G -orbits defined over \mathbb{F}_p . This of course does not resolve the question, but as Example 4.7 shows, any list of sufficient conditions is sure to be fairly restrictive.

Theorem 4.3 also provides a fairly accessible method for computing the number of G -orbits defined over \mathbb{F}_p . In section 6, we use Magma to count the number of GL_n -orbits in $\mathbb{E}(r, \mathfrak{gl}_n)$ for $n \leq 5$.

As mentioned in the introductory paragraph to this section, Theorem 4.3 follows from the previous sections and the following theorem of Lang.

Theorem 4.1 ([3], Theorem 2). *Let G be an algebraic group defined over a finite field F , and let V be a variety defined over F on which G acts morphically and transitively. Then V has an F -rational point.*

We should clarify that in Theorem 4.1, an action is transitive if there is a $v \in V$ such that $V = G \cdot v$. We do not require the map $G/G_v \rightarrow V$ to be an isomorphism of varieties. The proof of the following lemma is immediate from Theorem 4.1.

Lemma 4.2. *Let r be such that $\mathbb{E}(r, \mathfrak{g})$ is nonempty, and let \mathcal{O} be any G -orbit of $\mathbb{E}(r, \mathfrak{g})$. If \mathcal{O} is defined over \mathbb{F}_p , then the set of \mathbb{F}_p -rational points of \mathcal{O} is non-empty.*

Theorem 4.3. *Let G be connected and reductive, and let $p \geq h(G)$, p very good. The G -orbits of $\mathbb{E}(r, \mathfrak{g})$ defined over \mathbb{F}_p are in bijection with the G -conjugacy classes of elementary abelian p -groups of rank r in $G(\mathbb{F}_p)$. In particular, $\mathbb{E}(r, \mathfrak{g})$ contains finitely many G -orbits defined over \mathbb{F}_p . Furthermore, the number of \mathbb{F}_p -rational points of a G -orbit defined over \mathbb{F}_p is equal to the size of its corresponding G -conjugacy class.*

Proof. Let \mathcal{O} be any G -orbit of $\mathbb{E}(r, \mathfrak{g})$ defined over \mathbb{F}_p . By Lemma 4.2, $\mathcal{O}(\mathbb{F}_p)$ is non-empty. Furthermore, by Theorem 3.12, $\mathcal{O}(\mathbb{F}_p)$ is in bijective correspondence with a collection of elementary abelian p -subgroups of rank r in $G(\mathbb{F}_p)$. By G -equivariance, these elementary abelian p -subgroups form a G -conjugacy class. Conversely, starting with a G -conjugacy class of elementary abelian p -subgroups of rank r , Theorem 3.12 gives us a G -orbit of $\mathbb{E}(r, \mathfrak{g})$ whose \mathbb{F}_p -rational points correspond to elements of the given G -conjugacy class. \square

Question 4.4. If the number of conjugacy classes of $(\mathbb{Z}/p\mathbb{Z})^{\oplus r}$ in $G(\mathbb{F}_p)$ is the number of G -orbits of $\mathbb{E}(r, \mathfrak{g})$ defined over \mathbb{F}_p , what does the number of G -conjugacy classes of $(\mathbb{Z}/p\mathbb{Z})^{\oplus r}$ in $G(\mathbb{F}_q)$ represent when q is not a prime? Does it count the number of G -orbits defined over \mathbb{F}_q ?

Example 4.5. For an example illustrating that the reductive hypothesis may be unnecessary, consider the non-reductive group U_3 , the unipotent radical of B_3 , the group of upper triangular 3×3 matrices. Example 1.7 in [1] shows that $\mathbb{E}(2, \mathfrak{u}_3) \cong$

\mathbb{P}^1 . Explicitly, any elementary subalgebra has a basis of the form:

$$(4.5.1) \quad \left\{ \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & a & 0 \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix} \right\}$$

and this basis is unique up to scalar multiple of the vector (a, b) . A computation shows that each such subalgebra is fixed under conjugation by U_3 , so that the G -variety $\mathbb{E}(2, \mathfrak{u}_3) \cong \mathbb{P}^1$ has infinitely many G -orbits (each point is an orbit). However, only the \mathbb{F}_p -rational points of \mathbb{P}^1 , of which there are finitely many, are orbits defined over \mathbb{F}_p .

Example 4.6. Let $G = \mathrm{GL}_3$, $p \geq 3$, and $r = 2$. Any elementary subalgebra $\epsilon \in \mathbb{E}(2, \mathfrak{gl}_3)$ can be put in upper-triangular form, so ϵ is conjugate to a subalgebra ϵ' with basis given by (4.5.1) for some $[a : b] \in \mathbb{P}^1$. In general, the element $[a : b]$ is not defined by ϵ , as conjugating ϵ' by

$$\begin{pmatrix} \lambda & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \lambda \neq 0$$

gives an upper triangular subalgebra corresponding to $[\lambda a : b]$. It follows that all subalgebras $\epsilon \in \mathbb{E}(2, \mathfrak{gl}_3)$ that have an element of rank 2 are conjugate. The dimension of this orbit is shown to be 4 in example 3.20 of [1].

The only other subalgebras are those whose non-zero elements all have rank equal to 1. These subalgebras are conjugate to upper-triangular subalgebras corresponding to the points $[1 : 0]$ and $[0 : 1]$. These two upper-triangular subalgebras are not conjugate (in short, the conditions for a matrix A to conjugate $[1 : 0]$ to $[0 : 1]$ require that $\det(A) = 0$, a contradiction). The dimension of each of these two distinct orbits is 2 (Example 3.20, [1]). We have thus verified that $\mathbb{E}(2, \mathfrak{gl}_3)$ is the union of three GL_3 -orbits, all of which are defined over \mathbb{F}_p . As expected from Theorem 4.3, any elementary abelian p -subgroup of rank 2 in $\mathrm{GL}_3(\mathbb{F}_p)$ is conjugate to exactly one of the groups $\langle I + E_{12} + E_{23}, I + E_{13} \rangle$, $\langle I + E_{23}, I + E_{13} \rangle$, and $\langle I + E_{12}, I + E_{13} \rangle$. Here E_{ij} is the matrix whose only non-zero entry is a 1 in the i th row and j th column. This example will be further developed in Proposition 6.7 below.

Example 4.7. The following example showing that $\mathbb{E}(r, \mathfrak{g})$ may be an infinite union of orbits is due to R. Guralnick. Let $G = \mathrm{GL}_{2n}$ and let ϵ be the elementary subalgebra of $\mathfrak{g} = \mathfrak{gl}_{2n}$ of dimension n^2 whose matrices only have nonzero entries in the upper-right $n \times n$ block are zero. For any $r \leq n^2$, we have $\mathrm{Grass}(r, \epsilon) \subset \mathbb{E}(r, \mathfrak{g})$ so that $\dim(\mathbb{E}(r, \mathfrak{g})) \geq \dim(\mathrm{Grass}(r, \epsilon)) = (n^2 - r)r$. If r and n^2 are such that $(n^2 - r)r > 4n^2$, then $\dim(\mathbb{E}(r, \mathfrak{g})) > \dim(G)$, so that clearly $\mathbb{E}(r, \mathfrak{g})$ is not a finite union of G -orbits.

Question 4.8. As with nilpotent orbits of \mathfrak{g} , we can place a partial ordering on the G -orbits of $\mathbb{E}(r, \mathfrak{g})$ by $\mathcal{O} \leq \mathcal{O}'$ if and only if $\overline{\mathcal{O}} \subset \overline{\mathcal{O}'}$. For classical Lie algebras, the ordering on nilpotent orbits ($r = 1$) corresponds to the dominant ordering on Jordan type. For $r > 1$, given two G -conjugacy classes C and C' of elementary abelian p -groups of rank r in $G(\mathbb{F}_p)$ with corresponding orbits \mathcal{O} and \mathcal{O}' defined over \mathbb{F}_p , is there some group-theoretic condition on C and C' that determines when $\mathcal{O} \leq \mathcal{O}'$? In other words, can we describe the partial ordering on orbits in the group setting? Notice that the existence of a unique maximal element in the partial order implies

that $\mathbb{E}(r, \mathfrak{g})$ is irreducible. Describing the partial order in the group setting might allow us to find further examples of groups G such that $\mathbb{E}(r, \text{Lie}(G))$ is irreducible.

Example 4.9. For the case $G = \text{GL}_n$ and $r = 1$, the answer to Question 4.8 is already known. For each unipotent $g \in \text{GL}_n(\mathbb{F}_p)$, we know by the theory of Jordan forms that g is conjugate to a direct sum of Jordan blocks, all with eigenvalue 1. So as in the nilpotent case, the orbits are ordered by Jordan type of the corresponding unipotent elements. This is no surprise remembering that the nilpotent and unipotent G -varieties are isomorphic.

Remark 4.10. Example 4.9 suggest that the answer to Question 4.8 for classical Lie algebras may lie in the Jordan types of the elements of C and C' . That is, there is a condition on the Jordan types of elements in C and C' that determines when $\mathcal{O} \leq \mathcal{O}'$.

5. IRREDUCIBILITY OF $\mathbb{E}(r, \mathfrak{g})$

E. Friedlander has also asked for sufficient conditions such that $\mathbb{E}(r, \mathfrak{g})$ is irreducible. Here we use known results on the irreducibility of the commuting variety of nilpotent matrices to deduce irreducibility for $\mathbb{E}(r, \mathfrak{g})$.

Work of A. Premet in [7] shows that $\mathbb{E}(2, \mathfrak{gl}_n)$ is irreducible for all n . This is observed in Example 1.6 of [1]. Premet shows that under less restrictive hypotheses on \mathfrak{g} and p than we consider here, the variety of pairs of commuting nilpotent elements in \mathfrak{g} is equidimensional, whose irreducible components are in one-to-one correspondence with distinguished nilpotent orbits. For $\mathfrak{g} = \mathfrak{gl}_n$, there is only one distinguished nilpotent orbit, namely, the regular orbit. It follows that $\mathcal{C}_2(\mathcal{N}(\mathfrak{gl}_n))$ is irreducible. Since open sets of irreducible sets are themselves irreducible, and continuous images of irreducible sets are irreducible, the map of algebraic varieties $\mathcal{C}_2(\mathcal{N}(\mathfrak{gl}_n))^\circ \rightarrow \mathbb{E}(2, \mathfrak{gl}_n)$ discussed at the end of §1 shows that $\mathbb{E}(2, \mathfrak{gl}_n)$ is irreducible. This same argument shows that $\mathbb{E}(1, \mathfrak{g})$ is irreducible for all \mathfrak{g} , as the restricted nullcone $\mathcal{N}(\mathfrak{g})$ is irreducible.

It is also known that $\mathcal{C}_r(\mathcal{N}(\mathfrak{gl}_n))$ is irreducible for $r = 3$ and $n \leq 6$, and $r = 4$ and $n = 5$ ([10]), so by similar reasoning, it follows that $\mathbb{E}(r, \mathfrak{gl}_n)$ is irreducible for the corresponding pairs (r, n) . We should note that we have proven the implication

$$\mathcal{C}_r(\mathcal{N}(\mathfrak{g})) \text{ irreducible} \implies \mathbb{E}(r, \mathfrak{g}) \text{ irreducible}$$

however, the converse is not true. In Corollary 4 of ([10]) it is shown that $\mathcal{C}_4(\mathcal{N}(\mathfrak{gl}_4))$ is reducible, as well as $\mathcal{C}_r(\mathcal{N}(\mathfrak{gl}_n))$ for all $r \geq 5$ and $n \geq 4$, but Theorem 2.9 in [1] shows that $\mathbb{E}(n^2, \mathfrak{gl}_{2n})$ is irreducible for all n . We summarize the above discussion in the following theorem.

Theorem 5.1. *The variety $\mathbb{E}(r, \mathfrak{gl}_n)$ is irreducible for the following ordered pairs (r, n) : $(1, n)$ for any n , $(2, n)$ for any n , $(3, n)$ for $n \leq 6$, $(4, 5)$, and $(n^2, 2n)$ for any n .*

Question 5.2. The reducibility of the variety of r -tuples of pairwise-commuting matrices $\mathcal{C}_r(\mathfrak{gl}_n)$ and the variety of r -tuples of pairwise-commuting nilpotent matrices $\mathcal{C}_r(\mathcal{N}(\mathfrak{gl}_n))$ has been extensively studied. As we've already observed, since $\mathcal{C}_r(\mathcal{N}(\mathfrak{gl}_n))^\circ$ is open in $\mathcal{C}_r(\mathcal{N}(\mathfrak{gl}_n))$, the irreducibility of the latter implies that of the former. Are there counterexamples to the converse? Also, as in the case of $\mathcal{C}_r(\mathcal{N}(\mathfrak{gl}_n))$, is $\mathcal{C}_r(\mathcal{N}(\mathfrak{gl}_n))^\circ$ reducible for large enough r and n ?

Question 5.3. If $X \in \mathfrak{gl}_n$ is a regular nilpotent element and ϵ is the $n - 1$ -plane with basis given by $\{X, X^2, \dots, X^{n-1}\}$, is the orbit of X dense in $\mathbb{E}(n - 1, \mathfrak{gl}_n)$? Proposition 3.19 and Example 3.20 of [1] show that it is open in general and dense in the case $n = 3$. We have shown above that the question also has an affirmative answer for the cases $n = 4$ and $n = 5$. If the orbit of X is indeed dense, then $\mathbb{E}(n - 1, \mathfrak{gl}_n)$ is irreducible for all $n \geq 1$.

6. $\mathrm{GL}_n(k)$ -CONJUGACY CLASSES OF $(\mathbb{Z}/p\mathbb{Z})^{\oplus r}$ IN $\mathrm{GL}_n(\mathbb{F}_p)$

Since the G -orbits of $\mathbb{E}(r, \mathfrak{g})$ defined over \mathbb{F}_p are in bijection with the G -conjugacy classes of elementary abelian p -groups of rank r in $G(\mathbb{F}_p)$, we can count the number of G -orbits by computing in the finite group $G(\mathbb{F}_p)$. In this section we make some computations for $G = \mathrm{GL}_n$. The following results were computed using the ‘ElementaryAbelianSubgroups’ function in Magma. The computations below rely on Conjecture 6.1. For any algebraic group G defined over \mathbb{Z} , we denote by G_p the algebraic group defined by reducing the equations of $G \bmod p$.

Conjecture 6.1.

- (1) For G a connected, reductive algebraic group defined over \mathbb{Z} and for any pair of very good primes $p, q \geq h(G)$, there is a natural bijection between the d -dimensional G_p -orbits of $\mathbb{E}(r, \mathrm{Lie}(G_p))$ defined over \mathbb{F}_p and the d -dimensional G_q -orbits of $\mathbb{E}(r, \mathrm{Lie}(G_q))$ defined over \mathbb{F}_q . By natural, we mean the bijection is compatible for any triplet of primes p, q , and r .
- (2) Fix a very good prime $q \geq h(G)$ and a G_q -orbit of $\mathbb{E}(r, \mathrm{Lie}(G_q))$ of dimension d defined over \mathbb{F}_q , denoted \mathcal{O}_q . For all very good $p \geq h(G)$, let \mathcal{O}_p be the orbit in bijection with \mathcal{O}_q according to the bijection in (1). Then the counting function sending \mathcal{O}_p to $\#\mathcal{O}_p(\mathbb{F}_p)$ is a polynomial in p of degree d .

Table 1 below records experimental results for upper bounds on the number of GL_n -orbits of $\mathbb{E}(r, \mathfrak{gl}_n)$ defined over \mathbb{F}_p for varying r and n . In light of Conjecture 6.1, the primes used in the computation have been suppressed, although it is important to note that in all cases $p \geq n$. The numbers reported are upper bounds because it is not clear to the author how to determine when two $G(\mathbb{F}_p)$ -conjugate subgroups merge in some $G(\mathbb{F}_q)$. By Theorem 5.1, all the varieties represented here are irreducible, except for those corresponding to $(r, n) = (5, 5)$ and $(5, 6)$. $\mathbb{E}(6, \mathfrak{gl}_5)$ is known to be reducible, which follows from the fact that for $n > 1$, $\mathbb{E}(n(n + 1), \mathfrak{gl}_{2n+1})$ is the disjoint union of two connected components both isomorphic to $\mathrm{Grass}(n, 2n + 1)$ ([1], Theorem 2.10). It is not known to the author if $\mathbb{E}(5, \mathfrak{gl}_5)$ is irreducible. Table 2 records the dimension of the largest orbit from Table 1. In all known cases, this dimension is equal to the dimension of $\mathbb{E}(r, \mathfrak{g})$, suggesting the dimension of $\mathbb{E}(r, \mathfrak{g})$ may be determined by its largest orbit defined over \mathbb{F}_p .

Question 6.2. How can we construct a table similar to that of Table 1 which contains exact information, not just upper bounds? Also, can we expect a formula for the (r, n) entry of that table, or Table 2?

Example 4.9 shows that the entry in the n th row of column $r = 1$ in Table 1 is equal to $p(n) - 1$, where $p(n)$ is the number of partitions of the integer n . We lose the trivial partition $1 + 1 + \dots + 1 = n$ because this corresponds to the trivial subgroup. Example 4.9 also shows that the entries in column $r = 1$ are in fact

TABLE 1. Upper bounds for $|G\text{-orbits of } \mathbb{E}(r, \mathfrak{gl}_n) \text{ defined over } \mathbb{F}_p|$

n	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 5$	$r = 6$
2	1	0	0	0	0	0
3	2	3	0	0	0	0
4	4	10	8	1	0	0
5	6	35	67	32	5	2

TABLE 2. Dimension of largest orbit of $\mathbb{E}(r, \mathfrak{gl}_n)$ defined over \mathbb{F}_p

n	$r = 1$	$r = 2$	$r = 3$	$r = 4$	$r = 5$	$r = 6$
2	1	0	0	0	0	0
3	5	4	0	0	0	0
4	11	11	9	4	0	0
5	19	20	19	16	11	6

exact. For $r \geq 2$, we would need more exact data to determine if there is a closed formula for the number of orbits defined over \mathbb{F}_p . This closed formula may involve $p(n)$.

There is at least hope for an affirmative answer to Question 6.2 for Table 2, as evidenced by the following. Since $\mathbb{E}(1, \mathfrak{gl}_n)$ is the projectivized nullcone, the fact that the entries in column $r = 1$ are $n^2 - n - 1$ follows from the well-known formula $\dim(\mathcal{N}(\mathfrak{g})) = n^2 - n$. Furthermore, in Example 1.6 of [1] the authors use work of Premet in [7] to establish that the entries in column $r = 2$ are $n^2 - 5$, which agrees with our computation. Also in [1], the identifications of $\mathbb{E}(n^2, \mathfrak{gl}_{2n})$ with $\text{Grass}(n, 2n)$ and $\mathbb{E}(n(n+1), \mathfrak{gl}_{2n+1})$ with $\text{Grass}(n, 2n+1)$ give the following formulas (which agree with Table 2):

$$\dim(\mathbb{E}(n^2, \mathfrak{gl}_{2n})) = n(2n - n) = n^2$$

$$\dim(\mathbb{E}(n(n+1), \mathfrak{gl}_{2n+1})) = n(2n + 1 - n) = n(n+1)$$

The following proposition is another piece of evidence that the entries of Table 2 may have a closed form.

Proposition 6.3. *Let \mathcal{O} be the open GL_n -orbit of $\mathbb{E}(n-1, \mathfrak{gl}_n)$ containing the subalgebra ϵ spanned by the powers of a regular nilpotent element X (cf. [1], Proposition 3.19). Then $\dim(\mathcal{O}) = (n-1)^2$.*

Proof. Let $G = \text{GL}_n$. We will show the dimension of the stabilizer G_ϵ of ϵ has dimension $2n - 1$, from which we obtain:

$$\dim(\mathcal{O}) = \dim(G) - \dim(G_\epsilon) = n^2 - (2n - 1) = (n - 1)^2$$

We may choose X to be the Jordan block of size n with eigenvalue 0, so that G_ϵ consists solely of upper-triangular matrices. In this case, I claim that G_ϵ is isomorphic to the $(2n - 1)$ -dimensional quasi-affine variety defined by $x_1 \neq 0$, $x_2 \neq 0$ in \mathbb{A}^{2n-1} . The map defining the isomorphism is given by sending a matrix $A = (a_{ij})$ which normalizes \mathcal{O} to the point

$$(a_{11}, a_{22}, a_{12}, a_{23}, a_{13}, a_{24}, \dots, a_{1(n-1)}, a_{2n}, a_{1n})$$

For injectivity, we must show that the entries in the top two rows of A along with the condition $A \in G_\epsilon$ completely determine A . For surjectivity, we must show that any choice of entries in the top two rows of A define a matrix $A \in G_\epsilon$ as long as $a_{11} \neq 0$, $a_{22} \neq 0$ and $a_{21} = 0$.

What follows is rather tedious, but the basic idea is that the entries along a super-diagonal are determined uniquely by the first two entries in the super-diagonal, and these first two entries may be arbitrary (except in the case of the diagonal, in which case the entries must be non-zero). By a super-diagonal, we mean any collection of entries of the form $a_{i,j}$ where $j - i = k$ for some fixed $k = 1, \dots, n - 1$.

First, notice that $A \in G_\epsilon$ if and only if $AXA^{-1} \in \epsilon$. For $j > i$, the (i, j) entry of AXA^{-1} is

$$(6.3.1) \quad \frac{a_{ii}a_{i+1,j}}{a_{i+1,i+1}a_{jj}} - \frac{a_{i,i+1}a_{i+2,j}}{a_{i+2,i+2}a_{jj}} + \dots - \frac{a_{i,j-2}a_{j-1,j}}{a_{j-1,j-1}a_{jj}} + \frac{a_{i,j-1}}{a_{jj}}$$

We've assumed $i + j$ is odd, else we should switch the parity of all the signs. Notice that $a_{ii} \neq 0$ for all i as A is upper-triangular and invertible. For fixed $k = 1, \dots, n - 1$, the condition that $A \cdot X \cdot A^{-1} \in \epsilon$ requires that (6.3.1) is independent of choice of (i, j) such that $j - i = k$. For $j - i = 1$, (6.3.1) simplifies to

$$\frac{a_{ii}}{a_{jj}}$$

If this expression is to be independent of (i, j) such that $j - i = 1$, once we choose $a_{11} \neq 0$ and $a_{22} \neq 0$, then a_{ii} is determined for $i = 3, \dots, n$. For $k = 2, \dots, n - 2$, if (6.3.1) is independent of (i, j) such that $j - i = k$, then once we choose arbitrary $a_{1,k}$ and $a_{2,k+1}$, then $a_{i,k+i-1}$ is determined for $i = 3, \dots, n - k + 1$. Finally, a_{1n} does not appear in (6.3.1) for any (i, j) , so it may be chosen arbitrarily. This shows that A is uniquely determined by its top two rows (injectivity), and any choice of top two rows $a_{11} \neq 0$, $a_{22} \neq 0$ and $a_{21} = 0$ defines a matrix $A \in G_\epsilon$ (surjectivity). \square

Remark 6.4. A different approach to the computation in Proposition 6.3 was shown to the author by E. Friedlander and J. Pevtsova. They noticed that two regular nilpotent elements X and Y define the same orbit if and only if $Y = a_1X + a_2X^2 + \dots + a_{n-1}X^{n-1}$, with $a_1 \neq 0$. These $n - 1$ degrees of freedom together with the fact that the regular nilpotent orbit is $n^2 - n$ shows that the dimension of \mathcal{O} is $n^2 - n - (n - 1) = (n - 1)^2$.

If Question 5.3 has an affirmative answer, or if any subalgebra defined by a regular nilpotent element is in the orbit of largest dimension, then Proposition 6.3 computes the dimension of $\mathbb{E}(n - 1, \mathfrak{gl}_n)$ to be $(n - 1)^2$, which is verified through $n = 5$ in Table 2.

By considering a smaller subspace defined by a regular nilpotent element, the following proposition gives a lower bound on the dimension of $\mathbb{E}(r, \mathfrak{gl}_n)$ for the intermediate region $1 \leq r < n - 1$.

Proposition 6.5. *Let X be a regular nilpotent element in \mathfrak{gl}_n and for $1 \leq r < n - 1$ consider the elementary subalgebra $\epsilon_r = \text{Span}\{X, X^2, \dots, X^r\}$. Then $\dim(\text{GL}_n \cdot \epsilon_r) = n^2 - n - 1$. In particular, $\dim(\mathbb{E}(r, \mathfrak{gl}_n)) \geq n^2 - n - 1$ for $1 \leq r < n - 1$.*

Proof. I claim that the map sending a matrix $A \in G_{\epsilon_r}$ to $(a_{11}, a_{22}, a_{12}, a_{13}, \dots, a_{1n})$ is an isomorphism onto the quasi-affine variety in \mathbb{A}^{n+1} defined by the condition that the first two coordinates are nonzero. From this claim we have $\dim(\text{GL}_n \cdot \epsilon_r) = n^2 - (n + 1)$. The proof of the claim follows similar reasoning of the proof of

Proposition 6.3, except that the superdiagonals corresponding to $j - i = k > r$ must now be 0. It follows that $g \in G_{\epsilon_r}$ if and only if $g \in N_G(\text{Span}\{X\})$. To see this, note if $g \in N_G(\epsilon_r)$ and $gXg^{-1} = \sum c_i X^i$ with some $c_i \neq 0$ for $i > 1$, then $gX^r g^{-1}$ will have nonzero entries in the superdiagonal corresponding to $k = r + 1$. Hence, for $k > 1$ a choice of $a_{1,k}$ determines $a_{i,k+i-1}$ for $i = 2, \dots, n - k + 1$. For $k = 1$, we can still choose $a_{1,1}$ and $a_{2,2}$ arbitrarily. It follows that $\dim G_{\epsilon_r} = (n - 1) + 2 = n + 1$, so that $\dim(\text{GL}_n \cdot \epsilon_r) = n^2 - (n + 1)$. Notice we have shown that the corresponding bound on $\dim(\mathbb{E}(r, \mathfrak{gl}_n))$ is sharp in the limiting case $r = 1$. However, Table 2 shows that we may have strict inequality for $r = 2, \dots, n - 2$. \square

Motivated by Conjecture 6.1, we include two propositions computing the sizes of the different conjugacy classes found in Table 1.

Proposition 6.6. *There is one orbit in $\mathbb{E}(1, \mathfrak{gl}_2)$, and the number of \mathbb{F}_p -rational points is $p + 1$.*

Proof. A Sylow p -subgroup of $\text{GL}(2, p)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, so the Sylow theorems show there is a unique G -conjugacy class. One such group is represented by the matrices

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| a \in \mathbb{F}_p \right\}$$

whose stabilizer under conjugation is the group

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a, c \in \mathbb{F}_p^\times, b \in \mathbb{F}_p \right\}$$

This stabilizer has order $p(p - 1)^2$, so that the size of the orbit is

$$\frac{|\text{GL}(2, p)|}{p(p - 1)^2} = \frac{(p^2 - p)(p^2 - 1)}{p(p - 1)^2} = p + 1$$

The result then follows from Theorem 4.3. \square

Proposition 6.7. *There are three G -orbits in $\mathbb{E}(2, \mathfrak{gl}_3)$, two with $p^2 + p + 1$ \mathbb{F}_p -rational points, and one with $(p^2 + p + 1)(p + 1)(p - 1)$ \mathbb{F}_p -rational points.*

Proof. We know from Example 4.6 that there are 3 G -orbits of $\mathbb{E}(2, \mathfrak{gl}_3)$. The orbit consisting of subalgebras with elements of rank 2 has representative

$$E = \left\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle$$

in $\text{GL}_3(\mathbb{F}_p)$. The normalizer of E is

$$N_{\text{GL}_3(\mathbb{F}_p)}(E) = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \middle| af = d^2 \right\}$$

which has order $p^3(p - 1)^2$. Orbit-stabilizer then gives the size of the orbit:

$$\frac{|\text{GL}(3, p)|}{p^3(p - 1)^2} = \frac{(p^3 - p^2)(p^3 - p)(p^3 - 1)}{p^3(p - 1)^2} = (p^2 + p + 1)(p + 1)(p - 1)$$

The result for the large orbit follows from Theorem 4.3. The proof for the sizes of the other two conjugacy classes is similar, and omitted. \square

Notice that the dimensions computed in Example 4.6 and the degree of the polynomials in Proposition 6.7 provide evidence for the veracity of Conjecture 6.1.

Example 6.8. If Conjecture 6.1 is true, then a computation with Magma shows that $\mathbb{E}(3, \mathfrak{gl}_4)$ contains 8 G -orbits defined over \mathbb{F}_p of dimensions 3, 3, 6, 7, 7, 7, 8, and 9. The two orbits of dimension 3 must be closed, and by irreducibility, all orbits of degree less than 9 lie in the boundary of the orbit of dimension 9. Further understanding of the partial order on the orbits is necessary to determine which intermediate orbits lie in the closure of others. For example, is the orbit of dimension 6 closed, or is one or more of the 3 dimensional orbits found in its closure? Can this question be answered by some group theoretic condition on the G -conjugacy classes of subgroups corresponding to the orbits of dimensions 3, 3, and 6, per Question 4.8?

We conclude this example with the following table, which reports how many \mathbb{F}_p -rational points lie in each orbit.

TABLE 3. Orbits of $\mathbb{E}(3, \mathfrak{gl}_4)$ defined over \mathbb{F}_p

$\dim(\mathcal{O})$	$\#\mathcal{O}(\mathbb{F}_p)$
3	$(p^2 + 1)(p + 1)$
3	$(p^2 + 1)(p + 1)$
6	$(p^2 + p + 1)(p^2 + 1)(p + 1)^2$
7	$(p^2 + p + 1)(p^2 + 1)(p + 1)p(p - 1)$
7	$(p^2 + p + 1)(p^2 + 1)(p + 1)^2(p - 1)$
7	$(p^2 + p + 1)(p^2 + 1)(p + 1)^2(p - 1)$
8	$(p^2 + p + 1)(p^2 + 1)(p + 1)p^2(p - 1)$
9	$(p^2 + p + 1)(p^2 + 1)(p + 1)^2p(p - 1)^2$

REFERENCES

- [1] J. Carlson, E. Friedlander, J. Pevtsova, *Elementary subalgebras of Lie algebras*, preprint (2012).
- [2] J. Carlson, Z. Lin, D. Nakano, *Support varieties for modules over Chevalley groups and classical Lie algebras*, Trans. A.M.S. **360** (2008), 1870-1906.
- [3] S. Lang, *Algebraic groups over finite fields*, American Journal of Mathematics **78** (1956), 555-563.
- [4] M. Lincoln, D. Towers, *Frattini theory for restricted Lie algebras*, Archiv der Mathematik **45** (1985), 451-457.
- [5] G. McNinch, *Optimal $SL(2)$ -homomorphisms*, Comment. Math. Helv. **80** (2005), 391-426.
- [6] G. McNinch, *Abelian unipotent subgroups of reductive groups*, J. Pure and Applied Algebra, **167** (2002) 269-300.
- [7] A. Premet, *Nilpotent commuting varieties of reductive Lie algebras*, Invent. Math. **154** (2003), 653-683.
- [8] G. Seitz, *Unipotent elements, tilting modules, and saturation*, Invent. Math. **141** (2000), 467-502.
- [9] J. Serre, *Sur la semi-simplificité des produits tensoriels de représentations de groupes*, Invent. Math. **116** (1994), 513-530.

- [10] K. Sivic, *On varieties of commuting nilpotent matrices*, preprint (2013).
- [11] S. Smith, *Subgroup complexes*, Mathematical Surveys and Monographs, 179, American Mathematical Society 2011.
- [12] P. Sobaje, *Exponential maps, commuting nilpotent Varieties, and saturation*, preprint (2013).
- [13] P. Sobaje, *On Springer isomorphisms for groups of classical type*, preprint (2012).
- [14] D. Quillen, *The spectrum of an equivariant cohomology ring: I, II*, Ann. Math **94** (1971), 549-572, 573-602.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA
E-mail address: `hjewarner@usc.edu`